Assignment VI
Intrusion Detection Systems (IDS)
Intrusion Prevention Systems (IPS)
pfSense / OPNsense

S7 / S5 B.Tech: Computer Security Lab

Due Date: 04 November 2021 11:30 PM

1 Introduction

Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.

1.1 Problems IDS/IPS Address

A typical business network has several access points to other networks, both public and private. The challenge is maintaining the security of these networks while keeping them open to their customers. Currently, attacks are so sophisticated that they can thwart the best security systems, especially those that still operate under the assumption that networks can be secured by encryption or firewalls. Unfortunately, those technologies alone are not sufficient to counter today's attacks.

1.2 What Can You Do with IDS/IPS?

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators. In addition, some networks use IDS/IPS for identifying problems with security policies and deterring individuals from violating security policies. IDS/IPS have become a necessary addition to the security infrastructure of most organizations, precisely because they can stop attackers while they are gathering information about your network.

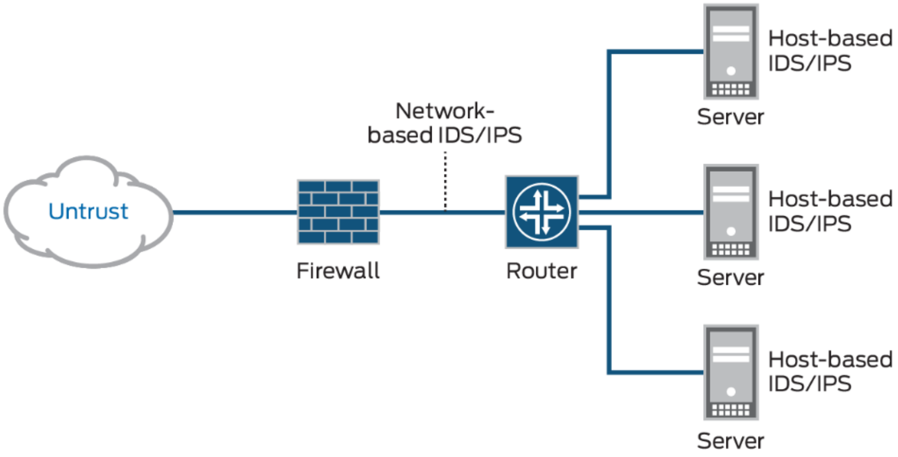

Figure 1: IDS / IPS Deployment

1.3 How Does IDS Work?

The three IDS detection methodologies are typically used to detect incidents.

- Signature-Based Detection compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.

- Anomaly-Based Detection compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.

- Stateful Protocol Analysis compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations.

2 Opensource IDS/IPS: Snort / Suricata / Zeek

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users. Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Suricata is the leading independent open source threat detection engine. By combining intrusion detection (IDS), intrusion prevention (IPS), network security monitoring (NSM) and PCAP processing, Suricata can quickly identify, stop, and assess the most sophisticated attacks. The Suricata project and code are owned and supported by the Open Information Security Foundation (OISF), a non-profit that is committed to keeping Suricata open source forever.

Zeek has a long history in the open source and digital security worlds. Vern Paxson began developing the project in the 1990s under the name “Bro” as a means to understand what was happening on his university and national laboratory networks. Vern and the project’s leadership team renamed Bro to Zeek in late 2018 to celebrate its expansion and continued development. Zeek is not an active security device, like a firewall or intrusion prevention system. Rather, Zeek sits on a “sensor,” a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic. Zeek interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system.

3 What you have to do?

You have to reuse the setup that you have implemented in Assignment 5, as shown in the network diagram.

1. Add an IP from your Bridged network and configure it as “Virtual IP”. Now Using NAT, setup the client system as Server, which is accessible from your Laptop host Operating System. In this process you are actually hosting an internal server to public domain using a Firewall. Make sure you configure your WAN Port with static IP Address with a subnet(anything between /24 to /30 based on your ISP Router settings), so that you would be able to configure the second IP address as Virtual IP and use it to access the internal DVWA Server. Also note that the management LAN is in series 192.168.2.0/24 the client systems are in the series 192.168.3.0/24.

2. Install package Sort / Suricata and configure it and load all required signatures by creating account in snort and also by downloading ET Signatures. initially configure it in non-blocking and alert mode in WAN Port. Make sure that it is fully configured and updated.

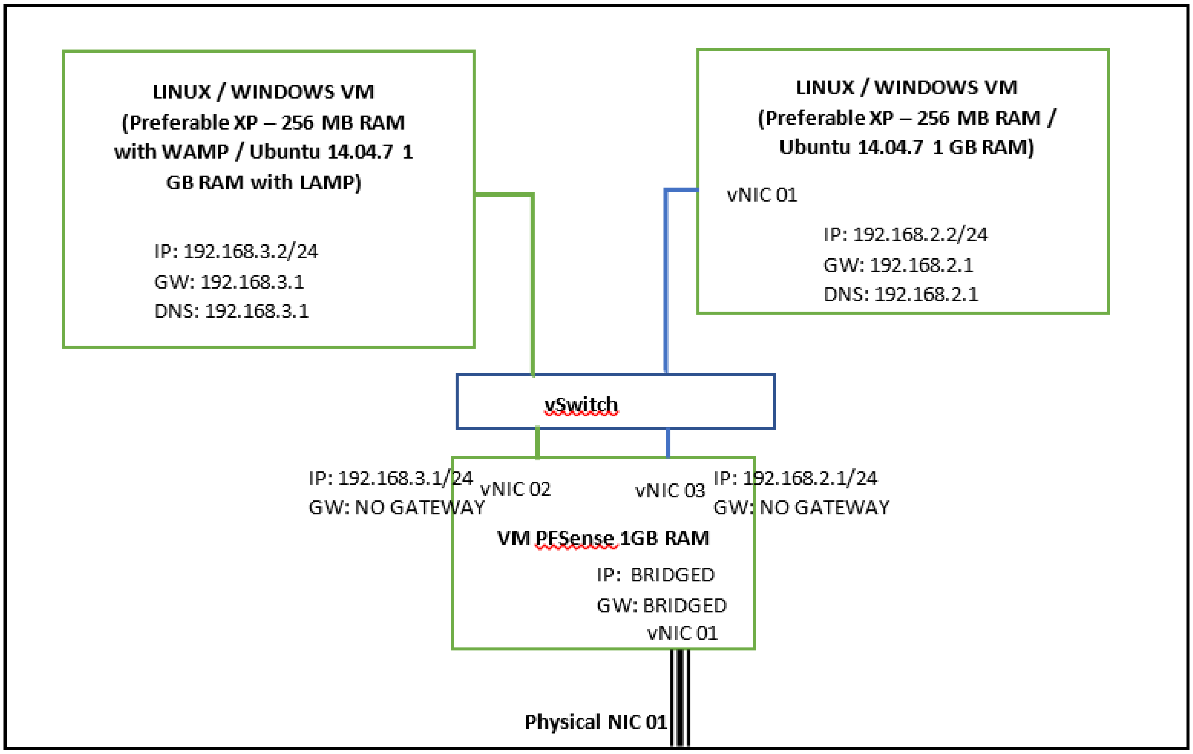

Figure 2: Network Diagram

3. Try to access the machine with IP Address 192.168.3.2 from the host Laptop, by using its NATed virtual IP Address. Execute the Web application attacks like SQL Injection, etc., on DVWA from your host laptop and make sure that the alerts are getting generated, but the statements are executed in the DVWA Server.

4. Now enable blocking mode (inline mode), so that the IP Addresses that are executing offensive activities are getting blocked by the IPS unit of the IDS.

   Now try to access the machine with IP Address 192.168.3.2 from the host Laptop, by using its NATed virtual IP Address. Execute the Web application attacks like SQL Injection, etc., on DVWA from your host laptop and make sure that the alerts are getting generated, packets are droped and IP Address is getting blocked. Confirm it by checking the blocked IP Addresses.

5. Please access the DVWA Machine (192.168.3.2) from 192.168.2.2 and do the same attack given in above step. Is it getting detected? Justify you findings.

6. Understand the signature of SNORT / Suricata and you should be able to write a new signature by yourself. Please write a signature to block the traffic that has pattern “HACKED”.

7. What do you mean by PCRE Scripts used for writing SNORT Rules. Will it be possible for writing the above rule? Please write the rule in PCRE Script format.

8. Now install and enable Zeek Package. Configure it.

9. Understand and explain its rules and demo on how you would be able to 1. customise, 2. disable a rule in Zeek.

4 What you have submit?

Google drive URL of a single recorded video. The video should be having demonstration along with your audio commentary, for each of the above task.

Any clarifications regarding the assignment has to brought to the instructor by 02/11/2021.

5 Readings

1. What is IDS and IPS?.

2. IDS vs IPS: Differences Between IDS and IPS.

3. IDS vs. IPS: What is the Difference?
4. Cyber Edu What is an Intrusion Prevention System (IPS)?
5. Differences Between IPS and Firewalls
6. Suricata
7. Snort 3 is available!
8. zeek